Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in this application:

Listing of Claims:

1. (Currently Amended) A method of distributing electronic media, the method comprising:

receiving a file at a user computing device, the file comprising an integral decryption engine and encrypted media content;

requesting a decryption key from a remote server;

receiving the decryption key from the remote server at the user computing device over a communication network, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key; and

responding to receipt of said decryption key from said remote server at the user computing device by:

decrypting said media content at the user computing device using said integral decryption engine and the decryption key

wherein receiving the file at the user computing device comprises receiving the file from a remote computer over the communication network that includes the remote server from which the decryption key is received but through a communication path that does not include the remote server from which the decryption key is received.

2. (Previously Presented) The method of claim 1, comprising, after decrypting the media content, viewing said media content by executing viewer software, the viewer software also integral with said file.

3. (Previously Presented) The method of claim 1, comprising, after decrypting the media content, viewing said media content by executing external viewer software linked to said file.

4. (Currently Amended) A method of managing distribution of proprietary electronic media, the method comprising:

receiving a single file at a user computing device, the single file comprising an integral decryption engine, encrypted media content and integral media playback software, the single file executable independently of other programs to:

obtain a decryption key from a remote server over a communication network, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key;

decrypt the media content using the integral decryption engine and the decryption key; and

view the media content using the integral media playback software

wherein receiving the single file comprises downloading said single file from a computer via the communication network;

wherein the communication network from which the single file is downloaded includes the remote server from which the decryption key is obtained; and

wherein downloading the single file from the computer via the communication network comprises downloading the single file from the computer through a communication path that does not include the remote server from which the decryption key is obtained.

5.-10. (Cancelled)

11. (Currently Amended) The method of claim ~~6~~ 4, wherein said remote server tracks a number of decryption keys relating to the single file that have been issued by the remote server.

12.-16. (Cancelled)

17. (Previously Presented) A method according to claim 35 wherein the file is executable independently of other programs and wherein generating the user key, requesting the decryption key, using the user key to decrypt the decryption key and decrypting the media content are accomplished by executing the file.

18. (Previously Presented) A method according to claim 17 wherein the file also comprises integral media player software and wherein executing the file also causes execution of the integral media player software and playback of the media content.

19. (Cancelled)

20. (Previously Presented) A method according to claim 2 wherein decrypting the media content and viewing the media content are accomplished without storing a decrypted copy of the

media content in memory accessible to a user of the user computing device.

21. (Previously Presented) A method according to claim 4 wherein decrypting the media content and viewing the media content are accomplished without storing a decrypted copy of the media content in memory accessible to a user of the user computing device.

22.-24. (Cancelled)

25. (Currently Amended) A method according to claim 1 wherein receiving the file at the user computing device comprises downloading the file from the remote computer using a peer to peer network, the ~~from a~~ remote computer ~~that is~~ different from the remote server from which the decryption key is received.

26. (Cancelled)

27. (Previously Presented) A method according to claim 1 comprising previewing a previewable portion of the media content prior to decrypting the media content using the integral decryption engine and the decryption key.

28. (Previously Presented A method according to claim 4 wherein the single file is executable to view the media content using the integral media playback software without storing a decrypted copy of the media content in memory accessible to a user of the user computing device.

29.-30. (Cancelled)

31. (Previously Presented) A method according to claim 4 wherein the remote server tracks a number of decryption keys relating to the single file that have been issued by the remote server.

32. (Cancelled)

33. (Previously Presented) A method according to claim 4 comprising previewing a previewable portion of the media content prior to decrypting the media content using the integral decryption engine and the decryption key.

34. (Previously Presented) A method according to claim 1 comprising generating the user key at the user computing device.

35. (Previously Presented) A method according to claim 34 wherein decrypting the media content at the user computing device using the integral decryption engine and the decryption key comprises using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.

36. (Previously Presented) A method according to claim 35 wherein using the user key to decrypt the decryption key is performed without storing the decrypted decryption key in memory accessible to a user of the user computing device.

37. (Cancelled)

38. (Previously Presented) A method according to claim 36 wherein decrypting the media content and viewing the media content are accomplished without storing a decrypted copy of the media content in memory accessible to a user of the user computing device.

39. (Cancelled)

40. (Previously Presented) A method according to claim 35 comprising previewing a previewable portion of the media content prior to decrypting the media content using the integral decryption engine and the decryption key.

41. (Currently Amended) A method according to claim 35 wherein receiving the file at the user computing device comprises downloading the file from the remote computer using a peer to peer network, the ~~from a~~ remote computer ~~that is~~ different from the remote server from which the decryption key is received.

42. (Previously Presented) A method according to claim 1 wherein decrypting the media content at the user computing device using the integral decryption engine and the decryption key comprises using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.

43. (Previously Presented) A method according to claim 4, wherein execution of the single file causes the user computing device to generate the user key at the user computing device.

44. (Previously Presented) A method according to claim 43 wherein execution of the single file to decrypt the media content using the integral decryption engine and the decryption key comprises using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.

45. (Cancelled)

46. (Currently Amended) A method of distributing electronic media, the method comprising:

receiving a file at a user computing device, the file comprising an integral decryption engine and encrypted media content;

generating a user key at the user computing device, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device;

requesting a decryption key from a remote server;

receiving the decryption key from the remote server at the user computing device over a communication network, the decryption key itself encrypted at the remote server with the user key such that the user computing device can use the user key to decrypt the decryption key; and

responding to receipt of said decryption key from said remote server at the user computing device by:

using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key at the user computing device; and

decrypting said media content at the user computing device using said integral decryption engine and the decrypted decryption key.

wherein receiving the file at the user computing device comprises receiving the file from a remote computer over the communication network that includes the remote server from which the decryption key is received but through a communication path that does not include the remote server from which the decryption key is received.

47. (Cancelled)

48. (Currently Amended) A method according to claim 1 comprising:

sending the file from the user computing device to a second user computing device over ~~a~~ the communication network over a second communication path that does not include the remote server;

upon receipt of the file at the second user computing device:

sending a request, from the second user computing device to the remote server, for the decryption key;

receiving the decryption key from the remote server at the second user computing device, the decryption key itself encrypted at the remote server with a second user key, the second user key bonded to the second user computing device by being based at least in part on one or more characteristics of the second user computing device such that the second user computing device can use the second user key to decrypt the decryption key; and

responding to receipt of the decryption key from the remote server at the second user computing device by decrypting the media content at the second user computing device using the integral decryption engine and the decryption key.

49. (Previously Presented) A method according to claim 48 comprising, after receiving the file at the second user computing device, generating the second user key at the second user computing device.

50. (Previously Presented) A method according to claim 49 wherein decrypting the media content at the second user computing device using the integral decryption engine and the decryption key comprises using the second user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.

51. (Cancelled)

52. (Currently Amended) A method according to claim 4 comprising:

sending the file from the user computing device to a second user computing device over ~~a~~ the communication network over a second communication path that does not include the remote server;

upon receipt of the file at the second user computing device:

sending a request, from the second user computing device to the remote server, for the decryption key;

receiving the decryption key from the remote server at the second user computing device, the decryption key itself encrypted at the remote server with a second user key, the second user key bonded to the second user computing device by being based at least in part on one or more characteristics of the second user computing device such that the second user computing device can use the second user key to decrypt the decryption key; and

responding to receipt of the decryption key from the remote server at the second user computing device by decrypting the media content at the second user computing device using the integral decryption engine and the decryption key.

53. (Previously Presented) A method according to claim 52 comprising, after receiving the single file at the second user computing device, generating the second user key at the second user computing device.

54. (Previously Presented) A method according to claim 53 wherein decrypting the media content at the second user computing device using the integral decryption engine and the decryption key comprises using the second user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.

55. (Previously Presented) A method according to claim 1 wherein the decryption key received at the user computing device is permanent such that decrypting the media content at the user computing device using the integral decryption engine and the decryption key may be performed multiple times at the user computing device using the integral decryption engine and the same decryption key.

56. (Previously Presented) A method according to claim 4 wherein the decryption key obtained at the user computing device is permanent such that subsequent executions of the single file decrypt the media content at the user computing device using the integral decryption engine and the same decryption key.

57. (New) A method according to claim 1 wherein the user key is based on a digital fingerprint of the user computing device.

58. (New) A method according to claim 4 wherein the user key is based on a digital fingerprint of the user computing device.